Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0147

Kwetsbaarheden verholpen in F5 BIG-IP

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-05-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

F5 heeft kwetsbaarheden verholpen in de BIG-IP systemen.

Duiding

De kwetsbaarheden bevinden zich in verschillende configuraties van de BIG-IP systemen, waaronder het Traffic Management Microkernel (TMM) dat kan worden beëindigd door ongepubliceerde verzoeken. Dit kan leiden tot prestatie- en stabiliteitsproblemen, vooral voor softwareversies die End of Technical Support (EoTS) hebben bereikt. De kwetsbaarheden kunnen ook leiden tot ongeautoriseerde toegang en privilege-escalatie voor gebruikers, wat de beveiliging van de systemen in gevaar kan brengen.

Oplossingen

F5 heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://my.f5.com/manage/s/article/K000139503
- https://my.f5.com/manage/s/article/K000140968
- https://my.f5.com/manage/s/article/K000150668
- https://my.f5.com/manage/s/article/K000140937
- https://my.f5.com/manage/s/article/K000137709
- https://my.f5.com/manage/s/article/K000150598
- https://my.f5.com/manage/s/article/K000140574
- https://my.f5.com/manage/s/article/K000139571
- https://my.f5.com/manage/s/article/K000140919
- https://my.f5.com/manage/s/article/K000149952
- https://my.f5.com/manage/s/article/K000148591

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-35995	8.7 HIGH
CVE-2025-36504	8.7 HIGH
CVE-2025-36525	8.7 HIGH

CVE-2025-36546	9.2 CRITICAL
CVE-2025-36557	8.7 HIGH
CVE-2025-41399	8.7 HIGH
CVE-2025-41414	8.7 HIGH
CVE-2025-41431	8.7 HIGH
CVE-2025-41433	8.7 HIGH
CVE-2025-46265	8.7 HIGH
CVE-2025-31644	8.5 HIGH

CWE's

CWE	Beschrijving
CWE-125	Out-of-bounds Read
CWE-404	Improper Resource Shutdown or Release
CWE-476	NULL Pointer Dereference
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-863	Incorrect Authorization
CWE-787	Out-of-bounds Write
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')

Getroffen producten

F5
BIG-IP

BIG-IP Next
BIG-IP Next CNF
BIG-IP Next SPK
F5OS - Appliance
F5OS - Chassis

Disclaimer